LISTING OF THE CLAIMS PER 37 C.F.R. §1.121

1. (Previously cancelled)
2. (Previously cancelled)
3. (Previously cancelled)
4. (Previously cancelled)
5. (Previously cancelled)
6. (Previously cancelled)
7. (Previously cancelled)
8. (Previously cancelled)
9. (Previously cancelled)
10. (Previously cancelled)
11. (Previously cancelled)
12. (Previously cancelled)
13. (Previously cancelled)
14. (Previously cancelled)
15. (Previously cancelled)
16. (Previously cancelled)
17. (Previously cancelled)
18. (Previously cancelled)
19. (Previously cancelled)
20. (Previously cancelled)
21. (Previously cancelled)
22. (Previously cancelled)

23. (Previously cancelled)

24. (Previously cancelled)

25. (Previously cancelled)

26. (Previously cancelled)

27. (Currently amended) An in-car video recording apparatus comprising:

a plurality of encryption and decryption key pairs, each of the plurality of encryption and decryption key pairs being assigned to a different individual;

a display means for displaying status information;

a video camera;

a microphone; and

a base unit coupled to the video camera, the microphone, and the display means, the base unit comprising:

a buffer and merge circuit functioning to merge the status information with the video data and buffer the resulting composite live digital data,

a compression circuit for compressing the composite live digital video data stored in the buffer and for compressing the audio data,

means for recording the compressed live digital data and the audio data onto a digital data recording medium, and

anti-tampering means for calculating a digital signature for the compressed live digital data and the audio data, and encrypting the digital signature with at least one of the plurality of encryption and decryption key pairs.

28. (Previously presented) The apparatus as recited in claim 27, wherein the base unit further comprises means for monitoring for occurrence of physical phenomenon which indicates that the encrypted digital signature has been improperly altered.

29. (Previously presented) The apparatus as recited in claim 27, wherein the base unit further comprises means for monitoring for occurrence of electrical phenomenon which indicates that the encrypted digital signature has been improperly altered.

30. (Cancelled)

31. (Previously presented) The apparatus as recited in claim 27, wherein the different individuals that are assigned the plurality of encryption and decryption key pairs comprise an individual selected from the group consisting of patrolmen, evidence officers, officers, and judges.

32. (Currently amended) The apparatus as recited in claim 27, wherein the base unit further comprises a key port for receiving by insertion a key chip having at least one ~~the plurality of encryption~~ of the plurality of encryption and decryption key pairs installed thereon.

33. (Previously presented) A system for tamper-proofing digital data, the system comprising:

in-car police patrol car video surveillance equipment for recording video signals and generating digital data having a digital signature therefrom;

a digital data recording medium for storing the digital data and the digital signature;

a plurality of encryption and decryption key pairs, each of the plurality of encryption and decryption key pairs assigned to a different individual; and

at least one controller for performing multiple encrypting and decrypting operations on the digital signature using at least one of the plurality of encryption and decryption key pairs.

34. (Cancelled)

35. (Previously presented) The system as recited in claim 33, wherein the different individuals that are assigned the plurality of encryption and decryption key pairs comprise an individual selected from the group consisting of patrolmen, evidence officers, officers, and judges.

36. (Previously presented) The system as recited in claim 33, wherein the at least one controller further comprises a key

port for receiving by insertion a key chip having at least one of the plurality of encryption key pairs installed thereon.

37. (Previously presented) The system as recited in claim 33, wherein the in-car police patrol car video surveillance equipment records audio signals and generates the digital data and the digital signature therewith.

38. (Previously presented) The system as recited in claim 33, wherein the in-car police patrol car video surveillance equipment records status information and generates the digital data and the digital signature therewith.

39. (Previously presented) A method for tamper-proofing digital data, the method comprising:

recording video and audio signals with in-car police patrol car video surveillance equipment;

generating digital data having a digital signature from the recorded video and audio signals;

storing the digital data and digital signature on a digital data recording medium;

assigning a plurality of encryption and decryption key pairs to different individuals; and

performing multiple encrypting and decrypting operations on the digital signature with at least one of the plurality of encryption and decryption key pairs.

40. (Previously presented) The method as recited in claim 39, further comprising recording the digital data and the encrypted digital signature on multiple recording mediums in the process of performing the multiple encrypting and decrypting operations on the encrypted digital signature.

41. (Previously presented) The method as recited in claim 39, further comprising monitoring for occurrence of physical phenomenon which indicates that the encrypted digital signature has been improperly altered.

42. (Previously presented) The method as recited in claim 39, further comprising monitoring for occurrence of electrical phenomenon which indicates that the encrypted digital signature has been improperly altered.

43. (Cancelled)

44. (Previously presented) A system for tamper-proofing digital data, the system comprising:

means for recording video and audio signals related to police surveillance;

means for generating digital data having a digital signature from the video and audio signals;

means for storing the digital data and the digital signature on a digital data recording medium;

a plurality of encryption and decryption key pairs, the plurality of encryption and decryption key pairs being assigned to different individuals; and

means for performing multiple encrypting and decrypting operations on the digital data with at least one of the plurality of encryption and decryption key pairs.

45. (Previously presented) The system as recited in claim 44, further comprising means for monitoring for occurrence of physical phenomenon which indicates that the encrypted digital signature has been improperly altered.

46. (Previously presented) The system as recited in claim 44, further comprising means for monitoring for occurrence of electrical phenomenon which indicates that the encrypted digital signature has been improperly altered.